SYMBOL	DESCRIPTION
$f(\ )$	ALICE'S AND BOB'S COMBINING FUNCTION
I_A, I_B	ALICE'S AND BOB'S DISCARDABLE INITIALIZATION VECTOR
K_A, K_B	ALICE'S AND BOB'S PRIVATE SESSION KEY
M_A, M_B	ALICE'S AND BOB'S PUBLIC KEY
N_A, N_B	ALICE'S AND BOB'S RANDOM NONCE FOR KEY VERIFICATION
N_A+1, N_B+1	MODIFIED (INCREMENTED) RANDOM NONCES
α, ß	ALICE'S AND BOB'S CONGRUENT EXPONENTIAL BASE; (ALICE'S AND BOB'S MODULO VARIABLE)
P_A, P_B	ALICE'S AND BOB'S SECRET PASSWORDS
R_A, R_B	ALICE'S AND BOB'S PRIVATE RANDOM NUMBERS
S_A, S_B	ALICE'S AND BOB'S HIGH-ENTROPY SECRET
$(Y)_X$	ENCRYPT CLEARTEXT, Y, WITH KEY X
$(Z)^{-1}{}_X$	DECRYPT CIPHERTEXT, Z WITH KEY X
$(N_B)\Sigma^{n}_{i=2}$	SUPERENCRYPT PLAINTEXT, N_B, WITH VARIABLE KEYS n

FIG. 1

200

Alice 202	XMSN 203	Bob 204
Generate R_A 206		Generate R_B 208
$M_A = \alpha^{R_A} \bmod ß$ 210		$M_B = \alpha^{R_B} \bmod ß$ 212
transmit M_A 214	214 →	$K_B = (M_A)^{R_B} \bmod ß$ 216
$K_A = (M_B)^{R_A} \bmod ß$ 220	← 218	transmit M_B 218
CONTINUE 222		CONTINUE 226
Encrypted Two way transmissions 224	230 ↔	Encrypted Two way transmissions 228

FIG. 2 *(Prior Art)*

300

Alice 202		XMSN 303	Bob 204	
Generate N_A 302			Generate N_B 304	
encrypt N_A as $(N_A)_{K_A}$ 306				
transmit $(N_A)_{K_A}$ 308		308 →	$N_A = ((N_A)_{K_A})^{-1}{}_{K_B}$ 310	
			increment N_A as N_A+1 312	
			encrypt $(N_B, N_A+1)_{K_B}$ 314	
N_B 320, N_A+1 322 = $((N_B, N_A+1)_{K_B})^{-1}{}_{K_A}$ 318		316 ←	transmit $(N_B, N_A+1)_{K_B}$ 316	
increment N_B as N_B+1 324				
encrypt $(N_B+1)_{K_A}$ 326				
transmit $(N_B+1)_{K_A}$ 328		328 →	$N_B+1 = ((N_B+1)_{K_A})^{-1}{}_{K_B}$ 330	
verify N_A+1 332			verify N_B+1 340	
If true, Bob 204 and Alice 202 share the same session key ($K_A = K_A$) CONTINUE 336	If false STOP 334		If false STOP 342	If true, Alice 202 and Bob 204 share the same session key ($K_A = K_A$) CONTINUE 344
Encrypted Two way transmissions 338		348 ↔	Encrypted Two way transmissions 346	

FIG. 3 *(Prior Art)*

400

Alice 402	XMSN 403	Bob 404
Store password P_A 406 and identity 408 410		Store password P_B 414 and identity 416 412
Generate N_A 418		Generate N_B 420
transmit identity 408, and service request 424 422	422 ---→	Obtain password P_B 414 and identity 416 from identity 408 424
		verify identity 408 = identity 416 426
		If true, Alice 403 is IDENTIFIED to Bob 404, CONTINUE 430 / If false STOP 428
encrypt N_B as $(N_B)_{P_A}$ 440	←--- 438	transmit N_B 438
transmit N_A 418, $(N_B)_{P_A}$ 440 442	442 ---→	verify $N_B = ((N_B)_{P_A})^{-1}{}_{P_B}$ 444
		If true, Alice 402 is AUTHENTICATED to Bob 404, CONTINUE 448 / If false STOP 446
		encrypt N_A as $(N_A)_{P_B}$ 450
verify $N_A = ((N_A)_{P_B})^{-1}{}_{P_A}$ 454	←--- 452	transmit $(N_A)_{P_B}$ 452
If true, Bob 404 is AUTHENTICATED to Alice 402, CONTINUE 458 / If false STOP 456		CONTINUE 462
Unencrypted Two way transmissions 460	466 ←→	Unencrypted Two way transmissions 464

FIG. 4

500

Alice 502	XMSN 503	Bob 504
Store password P_A 506 and identity 508 510		Store password P_B 514 and identity 516 512
Generate R_A 518		Generate R_B 522 and N_B 524 520
$M_A = (\alpha)^{R_A} \bmod ß$ 526		$M_B = (\alpha)^{R_B} \bmod ß$ 528
transmit identity 508, M_A 526, and service request 532 530	530 ---→	Obtain password P_B 514 and identity 516 based on identity 508 534
		verify identity 508 = identity 516 536
		If true, 544 Alice 502 is IDENTIFIED to Bob 504; CONTINUE / If false 538: 542 generate random P_B 542; CONTINUE / 540 STOP
		$K = K_B = (M_A)^{R_B} \bmod ß$ 546
		$S = S_B = f(P_B, M_A, M_B)$ 548
		encrypt N_B as $(N_B)_S$ 550
		encrypt $(N_B)_S$ as $((N_B)_S)_K$ 552
$K = K_A = (M_B)^{R_A} \bmod ß$ 556	←--- 554	transmit M_B, $((N_B)_S)_K$ 554
$S = S_A = f(P_A, M_A, M_B)$ 558		
$N_B = (((((N_B)_S)_K)^{-1}{}_K)^{-1}{}_S$ 560		
Generate N_A 562		
modify N_B as $N_{B_A}+1$ 564		
encrypt N_A, N_B+1 as $(N_A, N_B+1)_S$ ~ 566		
encrypt $(N_A, N_B+1)_S$ as $((N_A, N_B+1)_S)_K$ ~ 568		
transmit $((N_A, N_B+1)_S)_K$ 570	570 ---→	N_A 574, N_B+1 576 = $(((((N_A, N_B+1)_S)_K)^{-1}{}_K)^{-1}{}_S$ 572
		verify N_B+1 576 – 1 = N_B 524 578
		If true, Alice 502 is AUTHENTICATED to Bob 504; CONTINUE 580 / If false STOP 579
One way transmissions 582	582 ---→	Open one way link 581 / generate I_B 583

FIG. 5A

500

Alice 502	XMSN 503	Bob 504	
		If true, Alice 502 is AUTHENTICATED to Bob 504; CONTINUE 580	If false STOP 579
One way transmissions 582	582 →	Open one way link 581	generate I_B 583
		modify N_A as N_A+1 584	
		encrypt I_B, N_A+1 as $(I_B, N_A+1)_S$ 586	
		encrypt $(I_B, N_A+1)_S$ as $((I_B, N_A+1)_S)_K$ 588	
I_B 591, N_A+1 592 = $(((((I_B, N_A+1)_S)_K)-1_K)-1_S$ 590	589 ← - - -	transmit $((I_B, N_A+1)_S)_K$ 589	
verify N_A+1 592 – 1 = N_A 562 593		CONTINUE 597	
If true, Bob 504 is IDENTIFIED and AUTHENTICATED to Alice 502, CONTINUE 595	If false STOP 594		
Encrypted Two way transmissions 596	599 ↔	Encrypted Two way transmissions 598	

FIG. 5B

600

Alice 602	XMSN 603	Bob 604
Store password P_A 606 and identity 608 610		Store password P_B 614 and identity 616 612
Generate R_A 620 and N_A 622	618	Generate R_B 626 and N_B 628 624
$M_A = (\alpha)^{R_A} \bmod ß$ 630		$M_B = (\alpha)^{R_B} \bmod ß$ 632
encrypt N_A as $(N_A)_P$ 634		
transmit identity 608, M_A 630, $(N_A)_{P_A}$ 634, and service request 638 636	636 ---→	Obtain password P_B 614 and identity 616 based on identity 608 640
	642	verify identity 608 = identity 616
		If true, 650 Alice 602 is IDENTIFIED to Bob 604; CONTINUE If false 644: 648 generate random P_B 648; CONTINUE 646 STOP
		$N_A = ((N_A)_{P_A})^{-1}{}_{P_B}$ 652
		$K = K_B = (M_A)^{R_B} \bmod ß_B$ 654
		$S = S_B = f(P_B, M_A, M_B)$ 656
		modify N_A as $N_A + 1$ 658
	660	encrypt (N_B, N_A+1) as $(N_B, N_A+1)_S$
	662	encrypt $(N_B, N_A+1)_S$ as $((N_B, N_A+1)_S)_K$
$K = K_A = (M_B)^{R_A} \bmod ß$ 665	←664	transmit M_B, $((N_B, N_A+1)_S)_K$ 664
$S = S_A = f(P_A, M_A, M_B)$ 668		
N_B 672, N_A+1 674 = $(((((N_B, N_A+1)_S)_K)^{-1}{}_K)^{-1}{}_S$ 670		
verify N_A+1 674 – 1 = N_A 622	676	
If true, Bob 604 is IDENTIFIED and AUTHENTICATED to ALICE 502; CONTINUE 678 If false 677 STOP		
Open one way link 679	←680	One way transmissions 680
generate I_A 681		

FIG. 6A

600

Alice 602		XMSN 603	Bob 604
If true, Bob 604 is IDENTIFIED and AUTHENTICATED to ALICE 502; CONTINUE 678	If 677 false STOP		
Open one way link 679		680 ← - - -	Open one transmissions 680
generate I_A 681			
modify N_B as N_B+1 682			
encrypt I_A, N_B+1 as $(I_A, N_B+1)_S$ 683			
encrypt $(I_A, N_B+1)_S$ as $((I_A, N_B+1)_S)_K$ 684			
transmit $((I_A, N_B+1)_S)_K$ 685		685 - - - →	I_A $_B$ 687, N_B+1 688 = $((((I_A, N_B+1)_S)_K)-1_K)-1_S$ 686
CONTINUE 696			verify N_B+1 688 – 1 = N_B 628 690
			If true, Alice 602 is AUTHENTICATED to Bob 604, CONTINUE 693 / If 692 false STOP
Encrypted Two way transmissions 698		699 ← →	Encrypted Two way transmissions 694

FIG. 6B

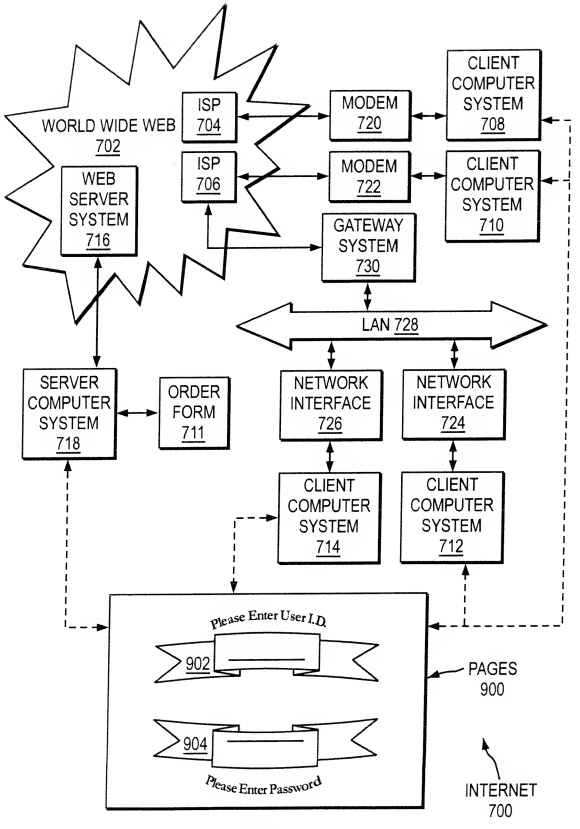
WORLD WIDE WEB
702
ISP
704
ISP
706
MODEM
720
MODEM
722
CLIENT
COMPUTER
SYSTEM
708
CLIENT
COMPUTER
SYSTEM
710
WEB
SERVER
SYSTEM
716
GATEWAY
SYSTEM
730
LAN 728
SERVER
COMPUTER
SYSTEM
718
ORDER
FORM
711
NETWORK
INTERFACE
726
NETWORK
INTERFACE
724
CLIENT
COMPUTER
SYSTEM
714
CLIENT
COMPUTER
SYSTEM
712
Please Enter User I.D.
902
904
Please Enter Password
PAGES
900
INTERNET
700

FIG. 7

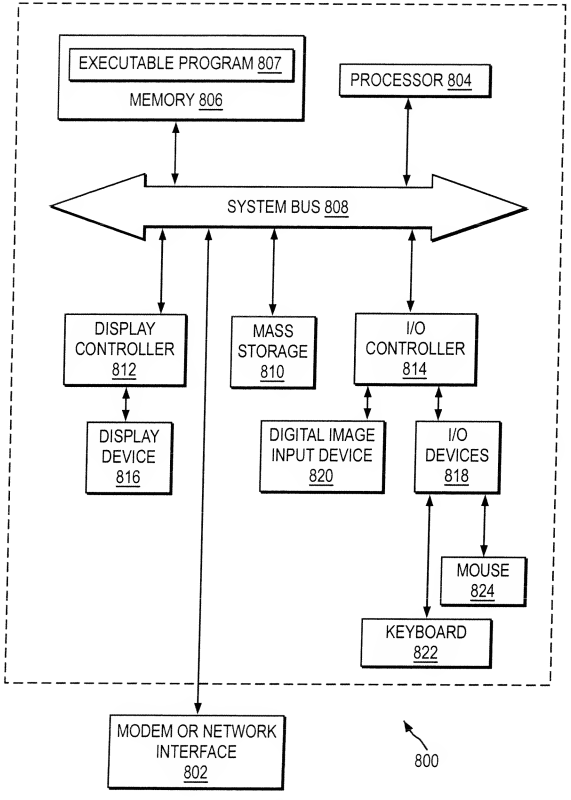
EXECUTABLE PROGRAM 807
MEMORY 806
PROCESSOR 804
SYSTEM BUS 808
DISPLAY CONTROLLER 812
MASS STORAGE 810
I/O CONTROLLER 814
DISPLAY DEVICE 816
DIGITAL IMAGE INPUT DEVICE 820
I/O DEVICES 818
MOUSE 824
KEYBOARD 822
MODEM OR NETWORK INTERFACE 802
800

FIG. 8